Dr. Anup Ghosh
Advanced Technology Office (ATO)
Information Assurance

As Tom suggested, the critical battlesphere today and in the future is information systems. And just as the Navy, Army, and Air Force have their traditional red spaces, the cyber battlesphere has its own red space.

In cyberspace, controlling the red space requires two capabilities: First, we must be able to observe and control the enemy's information systems. Second, we must build secure trustworthy systems that will form the backbone of all our military operations, both today and in the future.

It is no secret that America's economy, America's military, and America's national security all depend on information. Information that is routed through a highly interconnected network of critical infrastructures—a complex set of systems that are critical to running the nation's communications, financial, energy, and government sectors. The key enabling technology for all these complex systems is software. Software allows these systems to process information . . . to communicate . . . to carry out command and control functions. Software is one of the most sophisticated, most essential elements in our networks, but it is also one of the most vulnerable.

Today's software systems, with their millions of lines of code, are built with an architecture that resembles an elaborate house of cards, where a single programming or design flaw can undermine an entire system.

Consider the real-world ramifications of a few typical programming flaws. One typo that escaped detection in three lines of assembler code caused local telephone switches to fail in Washington, San Francisco, and Pittsburgh. Another minor coding flaw caused widespread disruption of AT&T's long-distance service. In 1998, according to press reports, an Aegis-class cruiser, the USS Yorktown, was engaged in training exercises off the coast of Norfolk, Virginia, when a divide-by-zero error crashed the software that ran the ship's propulsion system. The Yorktown was left dead in the water for hours.

Software flaws expose our systems to worms and viruses—such as Code Red, Nimda, and Flash Worms—that can saturate the Internet and cause grievous damage in a matter of minutes. They also make us vulnerable to information warfare or cyber attack.

Four years ago, in an exercise known as Eligible Receiver, DoD tested its ability to respond to an attack on our information infrastructure. Eligible Receiver revealed significant vulnerabilities and showed that we have little capability to detect or assess cyber attacks. Also in 1998, a major cyber attack was staged against Pentagon and DoD systems in what then-Deputy Secretary of Defense John Hamre called the "most concerted information warfare attack" against the Department of Defense. Afterward, we learned the attack had been launched by two California teenagers. The attack became known as Solar Sunrise.

My intention is not to criticize specific software systems or, in the case of the military, the dedicated men and women who manage them. But these problems vividly illustrate how fragile these systems are, how critical it is to protect them, and how short our current technology falls.

The need to guard software systems from a catastrophic attack has become an urgent priority at the highest levels of our Government. Earlier this year, Secretary Rumsfeld called the "leap into the information age" the "critical foundation of all our [military] transformation efforts." But he warned about the increasing danger of "cyber attacks on our information networks." He argued that terrorists and other enemies suspect that our "information networks, critical to our security and economy, are vulnerable" and he called protecting these networks from attack one of the Administration's key transformational goals.

America's continued military superiority is directly linked to information dominance. But as America's dependence on information systems grows, so does the potential for cyber attacks from sophisticated teams of engineers constructing stealthy, survivable worms that can take down entire information infrastructures and hinder our ability to respond to a national security crisis. The pervasive networking of software applications and devices, the ability to change functionality on the fly using mobile code, and the growing complexity of systems have created enormous obstacles to building secure, survivable, trustworthy systems—obstacles that challenge our traditional approaches to information assurance.

The core of the problem is this: Security has historically been an afterthought in designing software systems. That is what the Information Assurance Program is working to change. Our research focuses on three national-level concerns:

- Protection against denial-of-service attacks will give us the capability to operate in the face of distributed denial-of-service attacks our adversaries will launch in an attempt to deny us access to our computing resources when we need them most.

- Malicious code detection and containment will be a critical challenge in the future as our adversaries exploit systems on a large-scale in a small time frame through malicious software.

- Intrusion detection and response technologies that will provide us the ability to detect, respond to, and survive intrusions.

The Information Assurance Program has been making steady and significant progress in developing hardened, intrusion-tolerant systems; assurance methods and tools; and detection and response capabilities. Over the last year in the Operational Experimentation Program (or OPX), we've field-tested several new technologies to evaluate their performance and accelerate the transition to operational use. Let me outline a few briefly:

- Autonomic distributed firewalls, now known commercially as embedded firewalls, embed a firewall into every machine's network interface card and includes a management station that allows one administrator to control thousands at a time. Based in part on the promising results from the Fleet Battle Experiment India, as well as evaluations by other organizations, the Navy has launched a pilot program and budgeted funds to purchase and support these cards for years to come.

- Intrusion detection technologies—such as SPADE (or Statistical Packet Anomaly Detection Engine) and PHAD (Packet Header Anomaly Detection) engine—have proven successful at uncovering an assortment of stealthy aggressors that had been evading current defenses. These new systems have demonstrated a 20:1 improvement in data reduction on real military networks. SPADE has been incorporated into a recent upgrade to the Joint Intrusion Detection System. Operating system wrappers have thwarted effectively new forms of malicious code, leapfrogging the limitations of existing technologies that can detect only a list of known malicious codes.

- The Composable High Assurance Trusted Systems Program (or CHATS) is a nontraditional research initiative focused on making information security an integral part of open source operating systems. When we buy, develop, or install this software, we need better ways of knowing that it doesn't contain malicious code, accidental or deliberate security vulnerabilities, or other weaknesses. And we need tools to test their integrity. DARPA is working with several commercial partners to ensure the successful transition of the open source operating systems research.

- The Fault Tolerant Networks (FTN) Program is geared toward allowing vital networks to continue operating under partially successful attacks. We are developing technologies capable of thwarting and containing denial-of-service attacks, tracing attacks to their source, and helping the network recover and reconstitute itself to a fully operational level following an attack; in other words, a self-healing network.

These represent only a few of the winning information assurance technologies that have been tested successfully. They are only in the beginnings of the transition process from military to civilian applications. As we move forward with advanced research in information assurance, we confront a constantly changing landscape that is generating new challenges that require a new way of thinking beyond point solutions.

I'd like to discuss our ongoing research interests in three areas.

The first is the need to build trustworthy systems that provide the military with secure, robust, survivable platforms on which to base future mission-critical systems. Traditional information assurance solutions—including passwords, encryption, server configuration, and routers—do not address a fundamental cause of many security problems: bad software architecture, implementation, and policy. To break the cycle of penetrate-and-patch using temporary fixes and band-aids, we need to address the problem at its core by building systems that are designed to be secure, robust, survivable, and, in a word, trustworthy. To do so, we must fundamentally change the way we build software-intensive systems.

This effort starts by extending trust to program level objects and data structures. It includes research into dynamic assembly and configuration of certified operating system components. And it calls for security codesign to build security into systems from the development stage instead of after problems are discovered in the field. In many cases, the knowledge needed to build secure, trustworthy systems exists. We must convert that knowledge into practical tools that can give commercial developers the infrastructure to build trustworthy systems.

The second research focal point I would like to discuss is the threat of malicious code. Over the last 3 years, the intrusion threat to computer systems has changed dramatically. Instead of dealing primarily with individuals illegally hacking into the system, we are now faced with defending systems against a much more lethal threat: code-driven attacks.

How are code-driven attacks different? They can propagate autonomically. They can spread on a wide area network scale within hours and minutes rather than months and weeks. They can employ stealth and deception . . . be patient and survivable . . . exploit known vulnerabilities . . . and be dynamically programmable—all of which renders our traditional detection approaches obsolete.

Let me be blunt: Our critical infrastructures are vulnerable to code-driven threats. We're looking to the academic and commercial communities for research and insight into approaches to mitigate the cost and impact of large-scale malicious code attacks. Specifically, our goals are to:

- Build our understanding of infection factors and enhance our ability to quantify the rates and likelihood of success of code-driven threats.

- Anticipate the next generation of malicious code capabilities, including stealth, deception, data exfiltration, and systems that might disarm protections from the inside out.

- Develop malicious code countermeasures to mount effective defenses against code-driven attacks.

My third and final research focal point is the need to design and develop high assurance mobile applications. Computing is moving away from the desktop and the server to mobile, embedded computing devices. This is just as true in the battlesphere as it is in the office complex. Both commercial and military applications are creating a surge in demand for embedded computing devices and applications.

America's military of the future will rely on handheld devices to integrate laser range finding, GPS satellite positioning, and satellite voice and text messaging to relay information from the battlefield to control centers. Actually, that future is here. As the sophistication and mission-critical importance of mobile applications grows, our goal is to develop high assurance technology to protect applications and data that run and reside in tactical embedded systems. To meet this goal, we want to stimulate research for high assurance mobile applications including: device compromise detection, executable content control, data exfiltration monitoring, and secure device management.

Secretary Rumsfeld has urged America to adopt "a more entrepreneurial approach to developing military capabilities," an approach that encourages people to be proactive, to anticipate threats before they emerge.

I believe that philosophy is deeply embedded in DARPA's Advanced Technology Office. And I believe the work of the Information Assurance Program will play a critical role in securing America's military superiority.

Think of how a future enemy would attack America. No nation can compete with our firepower. No adversary can challenge our conventional forces. No foe can match our technological advantage. Instead they will attempt to cover our eyes . . . exploit our vulnerabilities . . . disrupt our dominance of the information sphere. Put differently, they'll try to develop a mathematical or code-driven "back door" to make our technology unworkable and useless.

This is one of the key asymmetric threats of the 21st century, and blunting that threat is the keystone of our mission in information assurance. By promoting new advances and harnessing technology, we can help our military leaders thwart the more sophisticated adversaries of the future, while providing high levels of information assurance to the warfighter in the battlesphere.

We have a lot of important work ahead, with extensive opportunities for research and development of new technologies. I look forward to your input, your insights, and your ideas.